THE HONORABLE ROBERT S. LASNIK

UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. PAIGE A. THOMPSON, Defendant.	Case No. CR19-159-RSL **AMAZON WEB SERVICES, INC.'S OPPOSITION TO DEFENDANT'S MOTION FOR EARLY RETURN OF TRIAL SUBPOENA** NOTE ON MOTION CALENDAR: January 20, 2022

INTRODUCTION

The Court should deny Defendant Paige Thompson's Motion for Early Return of Trial Subpoena ("Subpoena") to Amazon Web Services, Inc. ("AWS")[1]. As a result of good faith meet and confer efforts between AWS and Defendant, AWS has already produced a substantial amount of materials, including documents concerning AWS's investigation into Defendant's alleged intrusion into AWS customer accounts (including Capital One) (the "Incident"), testimony and interrogatory responses describing the Incident, and communications between the AWS security team and Capital One and other alleged victims about the intrusion. Defendant's present motion improperly seeks commercial contracts and billing information in an overbroad fishing expedition that will compromise confidential and commercially sensitive AWS information, while the documents she seeks cannot aid in her preparation for trial.

Defendant's motion concerns two of nine requests set forth in the Subpoena. Both requests fail to meet the *Nixon* standard for criminal discovery under Fed. R. Crim. P. 17, which requires

[1] AWS was incorrectly identified as "AWS Web Services, Inc." in the Subpoena. Dkt. 149.

that a defendant show relevancy, admissibility, and specificity. *See United States v. Nixon*, 418 U.S. 683, 699–700 (1974). First, Defendant requests "[*a*]*ny* contracts relating to cloud infrastructure and or/WAFs between" AWS and certain AWS customers ("victims") without any limitation of scope in time or subject matter. Dkt. No. 149-1, Ex. A, Request 8 (emphasis added). AWS's primary business is to provide services for cloud infrastructure; therefore all of its contracts with Capital One and the other victims identified in the Superseding Indictment would be responsive to the request. Second, Defendant requests "[a]ny bills and invoices for providing cloud infrastructure" sent from AWS to the victims over a two-year period. *Id.*, Ex. A, Request 9.

Defendant's motion merely describes the government's overarching theories and does not specify how the information sought could be relevant to Defendant's intent. Contracts, bills and invoices with AWS's customers, in existence with AWS customers at the time of the alleged hack, cannot answer the question of whether Defendant committed the crimes of which she is accused, or whether she had the intent to commit those crimes. In fact, the motion never attempts to explain the conclusory assertion that the Subpoena requests "are meant to get at issues in dispute with the government." *See* Dkt. 149 at 4. Instead, Defendant speculates that the "'value' of the information obtained, as well as any monetary 'loss'" (*id.* at 7–8) would be discernible from AWS's contracts, bills and invoices—without ever having seen those documents, and despite the parties' meet and confer discussions indicating otherwise. These requests constitute the kind of fishing expedition forbidden under Rule 17, *Nixon*, and its progeny.

This Court should deny the motion to compel in its entirety.

BACKGROUND

On November 24, 2021, Defendant issued AWS a trial subpoena under Fed. R. Crim. P. 17(c) requesting nine categories of documents. *See* Dkt. No. 149-1, Ex. A. After a lengthy meet and confer process, AWS agreed to produce information responsive to seven of the nine requests. *See* Dkt. 149 at 4. On January 12, 2022, AWS produced the documents that are potentially pertinent to Defendant's preparation for trial, including, but not limited to: 1) excerpts of corporate representatives' testimony from the related civil litigation on AWS's lack of knowledge of its

customers' WAF configurations for their AWS accounts; 2) documents, logs, and communications from within AWS's security organization concerning the root cause of the Incident—including documents showing the configurations exploited by Defendant and what she accessed in AWS customer accounts; 3) communications, reports, and notes (known as "tickets") created during the incident response team's investigation; 4) AWS's interrogatory responses in the related civil litigation, *In re: Capital One Consumer Data Breach Litigation*, MDL No. 1:19-md-02916 (AJT-JFA) (E.D. Va.),[2] describing the Incident and related AWS services; and 5) documents and communications with Capital One regarding a May 2019 note handed to an AWS employee that referenced a potential vulnerability associated with a specific IP address used by Capital One. Declaration of Tyler G. Newby in support of AWS's Opposition ("Newby Decl.") ¶ 6.

AWS was able to identify and produce these materials as the result of extensive discovery in the consumer class action against Amazon.com, Inc. ("Amazon") and Capital One concerning the Incident. As necessitated by the discovery proceedings in the civil matter, Amazon and AWS collected nearly 4.5 million files from more than 60 custodians and document repositories. *Id.* ¶ 3. Amazon reviewed and produced documents from current and former members of the account management team at AWS solely dedicated to the Capital One account, as well as employees of AWS's Professional Services organization and members of AWS's Security Operations team who responded to the Incident and provided support to Capital One and other impacted AWS customers. *Id.* ¶ 4. The documents AWS already produced in response to the Subpoena concern Defendant's intrusion; AWS's commercial contracts with and billings to Defendant's victims do not.

ARGUMENT

Federal Rule of Criminal Procedure 17(c) permits a defendant, with the Court's permission, to issue a subpoena to a witness to produce documents or data for trial. However, Rule 17(c) "was not intended as a discovery device," or to "allow a blind fishing expedition seeking unknown

[2] The undersigned is counsel of record for Amazon.com, Inc. and its wholly owned subsidiary AWS in the above-entitled action, MDL No. 1:19-md-02916. That class action was filed against Capital One and Amazon as a direct result of Defendant Paige Thompson's alleged acts of unlawfully accessing consumer data during the Incident. *See* Newby Decl. ¶ 2.

evidence." *United States v. Reed*, 726 F.2d 570, 577 (9th Cir. 1984). Under Rule 17(c), criminal subpoenas "must clear three hurdles: (1) relevancy; (2) admissibility; (3) specificity." *Nixon*, 418 U.S. at 700. This is an "exacting" standard and the burden falls on the party requesting the information. *Cheney v. United States Dist. Ct.*, 542 U.S. 367, 386 (2004). "[E]ach element must be shown with particularity and conclusory allegations are insufficient." *United States v. Estrada-Contreras*, No. CR17-301RSL, 2018 U.S. Dist. LEXIS 79302, at *2 (W.D. Wash. May 10, 2018) (citing *United States v. Eden*, 659 F.2d 1376, 1381 (9th Cir. 1981)); *see also United States v. Kilgore*, No. CR17-0203-JCC, 2019 WL 6913522, at *1 (W.D. Wash. Dec. 19, 2019) (denying motion for issuance of a subpoena *duces tecum* where Defendant failed to meet their burden by only making conclusory statements regarding the document's relevance to the defense).

Additionally, the Court must be persuaded that the moving party "cannot properly prepare for trial without such production and inspection in advance of trial and that the failure to obtain such inspection may tend unreasonably to delay the trial." *United States v. Krane*, 625 F.3d 568, 574 (9th Cir. 2010). And the Court may quash a subpoena for documents if their production would be "unreasonable or oppressive." Fed. R. Crim. P. 17(c)(2); *see also Nixon*, 418 U.S. at 698 (citing *Bowman Dairy Co. v. United States*, 341 U.S. 214 (1951)).

A. Defendant Has Not Met Her Burden under Rule 17(c).

Defendant's motion should be denied because her showing is wholly insufficient to meet the "exacting" standard under Rule 17(c). *See Cheney*, 542 U.S. at 386–87 (citing *Nixon*, 418 U.S. at 699). Defendant fails to establish that the requested documents are relevant, specific, or necessary for Defendant to prepare for trial. *See Kilgore*, 2019 WL 6913522, at *1 (citing *Nixon*, 418 U.S. at 699–700). Instead, the requests amount to a mere fishing expedition into highly sensitive commercial information in the hopes of "potentially" finding something relevant. *See Reed*, 726 F.2d at 577; *United States v. Mason*, No. CR 05-324-RE, 2008 WL 1909115, at *1 (D. Or. Apr. 25, 2008) ("The mere hope that the documents, if produced, may contain evidence favorable to the defendant's case is not sufficient."); *cf. Concord Boat Corp. v. Brunswick Corp.*, No. 96 C 6026, 1996 WL 705260, at *3 (N.D. Ill. Dec. 4, 1996) (denying motion to compel where

"[m]ere assertions of necessity" were insufficient to establish that the requested documents were relevant to the case).

First, Defendant's unsupported conclusions fail to explain how the requests at issue are relevant. Request 8 seeks "[a]ny contracts relating to cloud infrastructure and/or WAFs between" AWS and victims. Dkt. 149-1, Ex. A. As AWS is primarily in the business of providing cloud infrastructure services, this request seeks *every* contract between AWS and the victims. Defendant asserts that this request "will help explain, exactly, what kind of cloud infrastructure the alleged victims were renting from AWS." Dkt. 149 at 10. This explanation is insufficient under Rule 17 because it merely reiterates what documents Request 8 is seeking. Defendant is accused of exploiting a third-party web application firewall during the Incident, so any contracts pertaining to WAFs provided by AWS, which Capital One did not use, are irrelevant. And the notion that the "kind of cloud infrastructure" the victims were "renting" relates to Defendant's intent or whether she intruded into AWS's customers' accounts is non-sensical. Furthermore, whether the contracts contain any provisions regarding the respective responsibilities of AWS and its customers to secure their environments against malicious intruders is not relevant to whether Defendant intentionally accessed those accounts without authorization.

Defendant admits in her own motion that Request 8 will only "potentially" inform Defendant about "any limitations or configuration weaknesses about which AWS advised the victim entities." *Id.* That is, she speculates that the requested documents *might* help Defendant prepare for trial *if* there were any limitations or configuration weaknesses, *if* such notes were communicated to customers, and *if* that fact would be discernible from commercial contracts with customers (most likely not). The motion further states that Request 8 "may" also "shed light on whether the alleged victim entities, including Capital One, contemplated any type of 'value' associated with the[ir] data." *Id.* Defendant speculates that the commercial contracts would contain advice between the transacting parties. She fails to explain how such documents would have any bearing on the "value" of the type of data stored by customers across varied industries. *See Concord Boat*, 1996 WL 705260, at *3 (declining to compel broad requests for company's financial

documents when the movant failed to show how exactly the financials will help to establish the "relevant markets," a required element of every antitrust action). And, most importantly, Defendant fails to explain how that information would help her prepare for trial even if such information existed.

Defendant's conclusory explanations regarding Request 9 similarly fail. Request 9 seeks "bills and invoices for providing cloud infrastructure" to the victims over a two-year period. Dkt. 149-1, Ex. A. Defendant asserts that these documents are "directly relevant and admissible to the government's allegations of 'cryptojacking' and concomitant 'damage' to the victim entities." Dkt. 149 at 10. She provides no explanation, however, for how bills and invoices from the time period of the Incident (March to July 2019) could measure damages for the alleged cryptojacking or how she would be able to identify which charges are attributable to cryptocurrency mining malware versus other legitimate processing. *See* Dkt. 102 ¶¶ 1, 22, 24, 26, 28, 30, 32, 34 (alleging Thompson committed crimes between March and July 2019). Any damages calculation would require additional information, such as information from the victims regarding the regular use of their AWS services, and any fluctuations in their need for computing power during the months in question compared to the alleged dates of Defendant's illegal access. Defendant also fails to explain how bills and invoices from the remaining 19 months have a rational connection to the broad claim that these documents are "directly relevant" to the government's allegations. Defendant's arguments are based solely on speculation. *See Reed*, 726 F.2d at 577 ("Rule 17(c) [i]s not intended . . . to 'allow a blind fishing expedition seeking unknown evidence.'"); *see United States v. Avenatti*, No. (S1) 19 CR. 373 (PGG), 2020 WL 86768, at *7 (S.D.N.Y. Jan. 6, 2020) (denying request that a Rule 17(c) subpoena be issued, in part, because the request "relies on rank speculation").

Thus, Defendant has failed to establish the relevancy requirement with particularity as to Requests 8 and 9. *See United States v. Xiaoquing Zheng*, No. 1:19-CR-156, 2020 WL 6287481, at *7 (N.D.N.Y. Oct. 27, 2020) (denying requests where defendant failed to "offer any explanation as to how the terms of GE's non-disclosure agreements with its vendors are relevant to his defense"); *see also In re eBay Seller Antitrust Litig.*, No. C09-0735RAJ, 2009 WL 10677051, at *5 (W.D.

Wash. Aug. 17, 2009) ("[E]ven though the competitively sensitive documents [sought] might have some relevance, [Defendant] must do a substantially better job articulating their need for them.").

Second, Defendant's requests fail to meet the specificity requirement. For similar reasons as stated above, Requests 8 and 9 are overbroad as they reach beyond the scope of even potentially relevant information. *See Concord Boat Corp. v. Brunswick Corp.*, 169 F.R.D. 44, 50 (S.D.N.Y. 1996) (granting a motion to quash a subpoena, in part because, "[t]o the extent a subpoena sweepingly pursues material with little apparent or likely relevance to the subject matter it runs the greater risk of being found overbroad and unreasonable") (citation omitted); *United States v. Wittig*, 250 F.R.D. 548, 552 (D. Kan. 2008) ("A request will … be sufficiently specific where it limits documents to a *reasonable* period of time and states with *reasonable precision* the subjects to which the documents relate.") (emphases added). The majority of the information contained in the contracts, bills and invoices undoubtedly will be irrelevant to Defendant's purported theories of defense. *See Zheng*, 2020 WL 6287481, at *10 (denying overbroad request where it "would result in largely, if not exclusively irrelevant material"). Moreover, "'any and all' requests," such as Requests 8 and 9, "are particularly suspect in any Rule 17(c) analysis." *United States v. Collins*, No. 11-CR-00471-DLJ PSG, 2013 WL 1089908, at *4 (N.D. Cal. Mar. 15, 2013) (denying subpoena requests that were "enormous in scope" and requested "all" documents and communications relating to a cyber attack); *see also United States v. Reyes*, 239 F.R.D. 591, 606 (N.D. Cal. 2006) ("A demand for 'any and all documents relating to several categories of subject matter … , rather than specific evidentiary items,' suggests that the subpoena's proponent 'seeks to obtain information helpful to the defense by examining large quantities of documents, rather than to use Rule 17 for its intended purpose — to secure the production for a court proceeding of specific admissible evidence.'") (quoting *United States v. Louis*, No. 04–CR–203 (LTS), 2005 WL 180885, at *5 (S.D.N.Y. Jan. 27, 2005)); *United States v. Colima-Monge*, No. 96-CR-305-FR., 1997 WL 325318, at *5 (D. Or. June 6, 1997) (quashing request for "[*a*]*ny and all* records . . . setting forth guidelines, protocol, or other regulations promulgated *by any agency* concerning the operation of

ROCN agents and informants") (emphases in original). Therefore, Defendant's requests are also not sufficiently specific.

Finally, Defendant fails to explain why these documents are necessary to prepare for trial. AWS has produced a comprehensive set of documents, communications, testimony, and discovery responses related to Defendant's actions. Defendant makes no attempt to explain why or how the extensive information provided by AWS is insufficient. AWS has already provided the documents that bear any logical relationship to Defendant's potential defenses. *See Concord Boat*, 1996 WL 705260, at *3 (denying motion to compel documents to establish the "relevant market" in an antitrust suit because it is "not clear that [the movant] cannot glean the necessary information from the documents which it received from its other requests," and "there is no evidence that these documents are necessary in light of these other documents which were already produced").

Moreover, these requests involve highly sensitive AWS commercial information. *See In re eBay*, 2009 WL 10677051, at *4 ("The court must, in its sound discretion, balance the harm from disclosing the information, the requesting party's need for the information, and the effectiveness of possible safeguards for the information."). Here, Defendant seeks contracts, bills, and invoices containing commercially sensitive and confidential terms negotiated between AWS and its customers. Defendant fails to show any need that would justify the disclosure of such documents.

Accordingly, AWS respectfully requests that this Court deny the present motion because the requests are not relevant, specific, or necessary under Rule 17.

B. Defendant's Requests Are Unreasonable and Oppressive.

The Court may quash a subpoena for documents if their production would be "unreasonable or oppressive." *See Nixon*, 418 U.S. at 698 (citing *Bowman Dairy*, 341 U.S. 214); *see also United States v. Komisaruk*, 885 F.2d 490, 494-95 (9th Cir. 1989); Fed. R. Crim. P. 17(c)(2). Here, Defendant's requests regarding the contracts, bills and invoices are unreasonable and oppressive for two reasons.

First, as explained in section A above, Requests 8 and 9 seek irrelevant information and are an impermissible fishing expedition into AWS's confidential commercial relationships. The

blanket requests do not concern documents related to Defendant's guilt or intent, nor would the requested documents be useful at sentencing. This alone makes the requests unreasonable. *See United States v. Scovis*, 743 F. App'x 795, 800 (9th Cir. 2018) (holding that subpoena request was a fishing expedition where defendant "failed to make a showing of specificity or relevance"); *Avenatti*, 2020 WL 86768, at *6 (holding that an overly broad request constituted "the proverbial fishing expedition prohibited under the case law") (internal quotations omitted). Moreover, AWS has already produced documents that directly speak to the issues that Defendant identifies as relevant to her preparation for trial. *See supra* Sec. A; Newby Decl. ¶ 6. The information produced to Defendant was a result of AWS's enormous prior efforts in parsing out the documents relevant to the Incident following the collection of 4.5 million documents from more than 60 custodians and non-custodian repositories. Newby Decl. ¶ 3. Defendant's requests are unreasonable as Defendant makes no attempt to explain why the comprehensive information AWS has already provided does not suffice. *See In re eBay Seller Antitrust Litig.*, No. C09–735RAJ, 2009 WL 5205961, at *3 (W.D. Wash. Dec. 23, 2009) (quashing subpoena that sought confidential and sensitive business documents from Amazon because the information was, at best, marginally more valuable than what the issuing party already had in its possession).

Finally, Requests 8 and 9 are overly broad, rendering them oppressive and unreasonable. As explained above, Defendant does not attempt to narrow the scope of her blanket requests temporally or by subject matter. AWS further could not possibly "produce documents responsive to Subpoena Requests No. 8-9 . . . no later than seven days after the Court's entry of order." Dkt. 149 at 7. AWS has millions of customers and today offers "more than 200 fully featured services" for each customer. Newby Decl. ¶ 7. In order to respond to Defendant's requests related to contracts, bills and invoices between AWS and the victims, AWS would need to conduct an organizational-wide search, effectively replicating much of the same inquiry and collection performed in the consumer class action, not just for one customer (Capital One), but for nine others, each with its own dedicated account team. *Id.* ¶ 8. Given the volume of information sought, it would take weeks to comply with Defendant's requests, not the seven days suggested by Defendant.

Therefore, the Court should find Requests 8 and 9 unreasonable and oppressive. *Zheng*, 2020 WL 6287481, at *9, 11 (denying requests as unduly oppressive and unreasonable where compliance "would require an extensive investigation" and "result in producing an incredible amount of information regarding business transactions that Defendant had no role in").

CONCLUSION

For the reasons set forth above, AWS respectfully requests that the Court deny the motion to compel in its entirety.

Dated: January 14, 2021

Respectfully submitted,

FENWICK & WEST LLP

By: */s/ Brian D. Buckley*
Brian D. Buckley, WSBA No. 26423

1191 Second Avenue, 10th Floor
Seattle, WA 98101
Telephone: 206.389.4510
Facsimile: 206.389.4511
Email: bbuckley@fenwick.com

Tyler G. Newby (*pro hac vice* pending)

FENWICK & WEST LLP
555 California Street, 12th Floor
San Francisco, CA 94104
Telephone: 415.875.2300
Facsimile: 415.281.1350
E-mail: tnewby@fenwick.com

Counsel for Amazon Web Services, Inc.